

FILED ENTERED
LOGGED RECEIVED

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

NOV 08 2012

Purpose of the Affidavit

BY

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND

DEPUTY

1. This affidavit is made in support of the following: A search warrant for the residence located at 20 Montrose Road, Pasadena, Maryland 21122, hereafter referred to as the "Subject Premises" (as fully described in Attachment A and the attached photograph).
2. This affidavit is in support of an anticipatory search of the residence located in Attachment A. The residence is to be searched only after the parcel containing counterfeit goods (as more fully described herein) has been delivered and is physically present in the residence, and only after the parcel has been opened.
3. Based on the facts set forth in this affidavit, I respectfully submit there is probable cause to believe that there is presently concealed, and additional evidence will be present after the delivery contemplated here is accomplished in the Subject Premises, the items described in Attachment B hereto, all of which constitutes evidence, fruits, and instrumentalities, in violation of Title 18, United States Code, Section 545, which states in pertinent part:

Whoever knowingly and willfully, with intent to defraud the United States, smuggles, or clandestinely introduces or attempts to smuggle or clandestinely introduce into the United States any merchandise which should have been invoiced, or makes out or passes, or attempts to pass, through the customhouse any false, forged, or fraudulent invoice, or other document or paper; or whoever fraudulently or knowingly imports or brings into the United States, any merchandise contrary to law, or receives, conceals, buys, sells, or in any manner facilitates the transportation, concealment, or sale of such merchandise after importation, knowing the same to have been imported or brought into the United States contrary to law.

Title 18 United States Code Section 514, which states in pertinent part:

Whoever, with the intent to defraud - (1) draws, prints, processes, produces, publishes, or otherwise makes, or attempts or causes the same, within the United States; (2) passes, utters, presents, offers, brokers, issues, sells, or attempts or causes the same, or with like intent possesses, within the United States; or (3) utilizes interstate or foreign commerce, including the use of the mails or wire, audio, or other electronic communication, to transmit, transport, ship, move, transfer, or attempts or causes the same, to, from, or through the United States, any false or fictitious instrument, document, or other item appearing, representing, purporting, or contriving through scheme or artifice, to be an actual security or other financial instrument issued under the authority of the United States, a foreign government, a State or other political subdivision of the United States, or an organization, shall be guilty of a class B felony.

4. The information set forth below is based upon this affiant's personal observations or upon information provided to me by other law enforcement officers participating in the investigation as indicated. As the purpose of this affidavit is only to establish probable cause, your affiant has not set forth each and every fact known concerning this investigation.

Your Affiant

5. Your affiant, Joshua Gottschalk, is a Special Agent assigned to Homeland Security Investigations (HSI) under Immigration and Customs Enforcement (ICE) in Baltimore, Maryland and as such, your affiant is a law enforcement officer of the United States. Your affiant is presently assigned to the HIDTA Drug Money Laundering Initiative (DMLI) Group. During his tenure as an ICE/HSI Agent, your affiant has participated in numerous investigations involving smuggling narcotics, drug/money laundering conspiracies, and other unlawful activities. These investigations have included the use of surveillance techniques, Title III

Wiretaps, execution of search, seizure, and arrest warrants. Your affiant has attended the Criminal Investigator Training Program at the Federal Law Enforcement Training Center as well as Immigration and Customs Enforcement Special Agent Training. Your affiant is familiar with the facts and circumstances of the investigation that is the subject of this search warrant application. Your affiant has been employed with ICE since June of 2009.

Overview of Investigation

6. On or about October 18, 2012, Customs and Border Protection (CBP) Officers conducted an inbound customs examination of a Federal Express (FedEx) international package at their hub located in Memphis, Tennessee. CBP Officers selected the FedEx package ("the Parcel") with Airway Bill Number 800266222560 for examination. The airway bill number is an exclusive and unique identifying number used by FedEx to track individual packages. The Parcel was sent from Yinka Ogunjobi 55 Oba Ogunjobi Way, Lagos, Nigeria and addressed to Patricia Ridge at the Subject Premises.
7. CBP Officers opened the Parcel and discovered counterfeit United States Postal Service (USPS) money orders having a face value of \$433,392.91. According to CBP, the money orders were determined to be counterfeit based on their overall poor quality and lack of security features. United States Postal Service money orders are a form of financial instrument issued under the authority of the United States. The Parcel containing the counterfeit money orders was forwarded to HSI Agents in Baltimore for further investigation and a controlled delivery.

8. Public records show that the Subject Premises is owned and occupied by Doris M Cloud and Melissa A Thompkins. The couple has owned the Subject Premises since August 2011. HSI databases also identify Patricia Ridge as residing at the Subject Premises as recently as October 2012. A Maryland Judiciary Case Search of Patricia Ridge revealed her address as 20 Montrose Road, Pasadena, Maryland, 21122. Also included in the case search is a criminal charge of Assault-Sec Degree in December 2011 with no disposition rendered, a criminal charge of False Tax Return with a disposition of Nolle Prosequi in May 2012 a criminal charge of Tel Misuse: Repeat Calls with a disposition of Nolle Prosequi in September 2012.
9. On or about October 24, 2012, your affiant and other HSI members intend to deliver the Parcel to the Subject Premises in an undercover capacity. If the Parcel is accepted by anyone at the Subject Premises and is taken inside the residence and opened, your affiant and other law enforcement personnel are seeking permission to enter the target residence and search and seize the Parcel, as well as the items set forth in Attachment B.
10. A surveillance team of law enforcement officers is scheduled to follow the undercover agent as the agent attempts to deliver the Parcel to the residence. It has been my experience that visual surveillance alone of moving packages is difficult and not always successfully accomplished, due to the likelihood that the package will be opened in a nonpublic location, outside the view of law enforcement or the public.

11. It is important that investigators maintain some degree of control over the Parcel because the Parcel contains counterfeit money orders. In view of this and the difficulty in maintaining surveillance of the package and its contents, and because it is difficult to determine precisely when the intended recipients will open the package to retrieve its contents, HSI intends to install an electronic transponder inside the package. This is done to allow law enforcement officers to determine precisely when the package is opened. The transponder transmits a tone, but it does not monitor or record sounds. In the event that the package is opened, the transponder will set off an alarm tone, which will be transmitted to a receiver in the possession of law enforcement. This alarm will notify law enforcement that the package has been opened. Because the package may be opened in private areas, authority is sought to monitor the signal in all such areas to determine if and when the package is opened. Visual surveillance will enable law enforcement to determine the specific location where that package is delivered.
12. Based on my training knowledge and experience, intended recipients and senders of counterfeit monetary instruments and other illegal commodities smuggled into the United States, often check the status of the shipment by tracking the parcel's progress via the internet. Like almost all other shipping companies, FedEx offers such a service. According to the tracking data on the FedEx's website, the Parcel is shown to be in transit. The Parcel has been in the possession of the government since October 19, 2012. In order to ensure a successful controlled delivery, it is vital that law enforcement attempt and deliver the Parcel in a timely manner.

13. After the Parcel is delivered to the Subject Premises, and is opened, the residence will contain evidence pertaining to the smuggling and possession of counterfeit money instruments. At that time, probable cause will exist to search the Subject Premises to seize that evidence and to conduct a search for the items set forth in the Attachment B. If the package is not accepted, the warrant will not be executed and the package will remain in the custody of law enforcement.
14. Based on my experience and information that your affiant has obtained from others experienced in the investigation of counterfeiting and uttering counterfeits, I know that evidence of these crimes may include various pieces of computer hardware, computer software, computer storage media, computer records, and products purchased with counterfeit.
15. Based on previous investigations conducted by your affiant, she knows that recipients of large quantities of counterfeit monetary instruments are involved in African based internet scams intended to defraud individuals of legitimate funds. Specifically, these scams, which are sometimes referred to as "419 or Yahoo scams," involve over-invoicing or double invoicing of products listed for sale on the internet through such services as Craigslist and Yahoo. Individuals selling items on websites like Craigslist and Yahoo are contacted by individuals running the scam, who act as potential "buyers". The "buyer" will oftentimes send emails offering to pay more than the asking price if the seller provides a shipping payment or some other form of an advance fee. Once the agreement is in place, the "buyer," who is often physically located overseas in such countries as Nigeria and Ghana promises to send the seller a money order or a bank check to include

the extra amount or "shipping fees." The promised funds, which are counterfeit, are then sent through individuals living in the United States in order to legitimize the payment. These individuals are the distribution centers for such organizations sending countless counterfeit payments throughout the United States. These distribution centers are also involved in receiving the advance fees and transferring the funds overseas to where the "buyers" are located. The individuals operating as distribution centers receive directions, names and address of the intended scam victims via email from the "buyers," oftentimes over the internet or through the use of email.

16. Your affiant also knows that when an individual uses a computer to communicate over the internet, to send and receive email, or to store and reproduce financial documents, the computer will generally serve both as an instrumentality for committing the crime, and also as a storage device for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage device for evidence of the crime because individuals involved in such counterfeiting schemes usually maintain records and evidence relating to their crimes on their computers.
17. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of computers, your affiant knows that computer data can be stored on a variety of systems and storage devices. Your affiant has also learned that, even though computer files regarding the counterfeiting scheme may be deleted by the subjects


or others, the computer system that was previously used to store those files often retains evidence of the offense. This is because files deleted by the user may still remain (in whole or in part) on the storage media, as deletion of a file may not remove that data completely from the media. Your affiant also knows that during the search of the premises it is rarely possible to complete on-site examination of computer equipment and storage devices for a number of reasons, including the following:

- a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are many types of computer hardware and software in use today. It is often not possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.
- b. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover hidden, mislabeled, deceptively-named, erased, compressed, encrypted, or password-protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

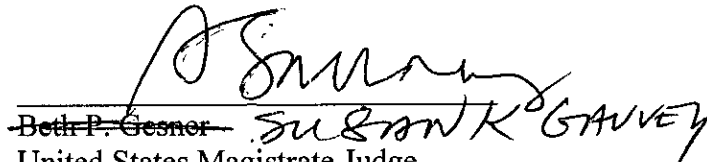
- c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in desktop computers are capable of storing millions of pages of text.
 - d. The ability to encrypt data also can complicate the mere mirroring of hard drives on site, since recreating the data may require the exact same hardware setup to function properly. It is, therefore, often necessary to reconnect all the original hardware and software in a controlled computer laboratory setting in order to retrieve the relevant evidence and data accurately.
18. Accordingly, because of the volume of data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting.
19. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in forensic examination of computers, your affiant is aware that searches and seizures of evidence from computers taken from the premises also commonly require agents to seize most or all of a computer system's input/output and peripheral devices. This is done so that qualified computer experts can accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the premises, in order to fully retrieve data from a

- computer system, investigators may need to seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, and are not otherwise seizable, such materials and/or equipment will be returned within a reasonable time.
20. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file directories and the individual files that they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer capable of containing pertinent files, in order to locate the evidence authorized for seizure by the warrant); examining all the structured, unstructured, deleted, and overwritten data on a particular piece of media; opening or reading the first few pages of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic key-word searches through all electronic storage areas to determine whether occurrences of such language contained in the storage areas are intimately related to the subject matter of the investigation.
21. Based upon the foregoing, in anticipation that the Parcel will be delivered and opened at the target residence, your affiant believes that probable cause will exist

to search the target residence, 20 Montrose Road, Pasadena, Maryland 21122 for evidence pertaining to the smuggling and possession of counterfeit monetary instruments in violation of 18 U.S.C. Sections 514 and 545.


Joshua Gottschalk
Special Agent
Homeland Security Investigations

Sworn to and subscribed by me this ²⁴ ~~15~~ day of ^{October} ~~August~~, 2012


~~Beth P. Gesner~~ ^{SUBANK GAVVEY}
United States Magistrate Judge

ATTACHMENT A

The address is a grey two story single family residence with grey siding and burgundy shutters. The front entrance to the residence has a white storm door and covered porch with grey support posts. The front steps to the residence have a black metal hand rail on both sides. The numerals "20" are displayed in black on a white background on a lamp post directly in front of the residence.



gme

ATTACHMENT B

Items to be seized are more fully described as follows:

1. Counterfeit items relating to this crime, including counterfeit or fraudulent USPS money orders or other financial instruments.
2. Shipping documents related to this crime, including FedEx receipts, shipping documentation, labels, boxes, packaging and bills of lading.
3. Documents, papers or correspondence relating to the sender of the subject Parcel, Yinka Ogunjobi or from the location of 55 Oba Ogunjobi Way, Lagos, Nigeria, or other locations in Nigeria or Ghana.
4. Bank account records, ^{fr}wire transfer records, bank statements, safe deposit box keys and records, money wrappers, rubber bands, money containers, financial records and notes from January 2012 to the present, showing payment, receipt, concealment, transfer, or movement of money; ONLY AS RELATED TO PATRICIA RIDGE *JA* *pm*
5. Personal telephone records, address books, telephone bills, documents, computer devises such as "Palm Pilots" and other items reflecting names, addresses, telephone numbers that document association; ONLY AS RELATED TO PATRICIA RIDGE *JA* *pm*
6. Photographs, letters, cables, telegrams, facsimiles, Federal Express and other shipping receipts and invoices, personal notes and documents and other items that ONLY AS RELATED TO PATRICIA RIDGE *JA* *pm*
7. Records of off-site locations to store records, including but not limited to safe deposit box keys, records, receipts, and rental agreements for storage facilities from January 2012 to the present; ONLY AS RELATED TO PATRICIA RIDGE *JA* *pm*

8. Records of mail and communications services from January 2012 to the present, cellular phones, text pagers, and other communication devices, including transaction and billing records maintained by service providers; *ONLY AS RELATED TO PATRICIA RHOGE*
9. Records, items and documents from January 2012 to the present reflecting travel, including passports, airline tickets, vehicle rental receipts, credit card receipts, hotel and restaurant receipts, cancelled checks, maps, and records of long distance calls, which reflect domestic and foreign travel; *ONLY AS RELATED TO PATRICIA RHOGE* *my* *JA*
10. Currency in an amount of ~~\$5,000.00~~ ^{10,000.00} or more, money wrappers, rubber bands, and devices used to count money; *AS IDENTIFIED TO PATRICIA RHOGE* *my* *JA*
11. Indicia of occupancy, residency or ownership of the premise described in this warrant, including utility bills, telephone bills, loan payment receipts, rent receipts, trust deeds, lease or rental agreements, addressed envelopes, escrow documents, keys, and bank account records. *ONLY AS RELATED TO PATRICIA RHOGE* *my* *JA*
12. Any and all information and/or data stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer or with the aid of computer related equipment. This media includes network servers, back-up tapes and diskettes, hard drives, floppy diskettes, fixed hard disks, removable hard disk cartridges, tapes, laser disks, video cassettes and other media which is capable of storing magnetic coding.
13. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, video recording devices, video recording players, monitors, and or televisions, flatbed scanners, and data where instrumentalities of and will contain evidence related to this crime.

14. Computer equipment and the related instructions and manuals.

Definitions

The following definitions apply to the terms as set out in this affidavit and attachment:

- a. Computer hardware

Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data-processing devices (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

- b. Computer Software

Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

- c. Documentation

Computer-related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices

Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha-numeric characters) usually operates a sort of digital key to unlock particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates test keys or hot keys, which perform certain pre-set security functions when touches. Data security software or code may also encrypt, compress, hide, or booby-trap protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

e. Records:

Includes all forms of documentation, including handwritten, typed, computer-generated, floppy disc, readable-writeable compact disc, computer paper, magnetic tape, microfilm or other medium including desktop and laptop computers with internal and/or external hard drives, zip drives, and other hardware, including scanners, necessary to access or to print such files).

Search Methodology

15. The computer hardware and software may be searched for the following items:

Any of the items described in paragraphs 1 through 11 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including floppy diskettes, fixed hard disks, or removable hard disk cartridges, software or memory in any form.

The search procedure of the electronic data contained in computer operating software or memory devices shall include the following techniques which shall be used to minimize the risk that those conducting the search will view information not within the scope of the warrant:

- a. Surveying various file directories and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. Opening or cursorily reading the first few pages of such files in order to determine their precise contents;
- c. Scanning storage areas to discover and possibly recover recently deleted files;
- d. Scanning storage areas for deliberately hidden files; or
- e. Performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.
- f. If after performing these procedures, the directories, files or storage areas do not reveal evidence of false or fraudulent identity documents or other criminal activity, the further search of that particular directory, file or storage area, shall cease.